KnowledgeFlow Data Security FAQs

1. Data Protection and Storage

Question	**Answer**
How is customer data protected at rest and in transit?	Data at rest is automatically encrypted when persisted to the cloud using Azure Open AI services. Data in transit is protected using HTTPS, encrypting all data passing between the browser and server using TLS.
What encryption standards are used?	TLS and Azure Open AI services.
Do you use end to end encryption and how are encryption keys managed?	End to end encryption is via SSL when users access data via the web app.
Is access controlled by System Admins based on least privilege?	Role-based least privilege access is configured and monitored daily for activity.

2. Compliance and Certifications

Question	**Answer**
What compliance certifications or frameworks do you adhere to?	Cyber Essentials Plus, ISO 27001 and ISO 47001.
Are these certifications validated through third-party audits?	Yes (Cyber Essentials – IASME, ISO – Citation).
Are you happy to provide evidence of certification?	Certainly, please email info@leadingai.co.uk requesting this information.

3. Identity and Access Management

Question	**Answer**
How do you manage identity and access control?	The web app provided to the client is protected by authentication and housed in their tenant; The client can control access via user groups.
Do you support SSO, MFA, RBAC, and least privilege principles?	Our preferred method is to build the product within your existing Microsoft Azure Tenant which benefits

	from whichever authentication your organisation deems best (e.g., 2-Factor Authentication). However, we are happy to discuss other implementations (e.g. hosting on our secure tenant.)
How is user provisioning and deprovisioning handled?	Clients can determine who has access to the web app. User groups can be created and applied within Azure. Provisioning and deprovisioning is handled by the customer in this instance which simplifies the process of maintenance.

5. Infrastructure Security and Monitoring

Question	**Answer**
How is your infrastructure monitored and protected against threats?	Security logs detailing logins are collected. Web app updates are applied monthly (or when required). Azure updates are automatically applied.
Do you use intrusion detection systems (IDS), SIEM tools, and conduct regular vulnerability assessments?	The app is hosted in the customers Azure tenant and inherits your existing security layer. Regular assessment of the codebase and updates are made when required.

6. Vulnerability Management

Question	**Answer**
How quickly do you patch known vulnerabilities (e.g., CVEs)?	Core known vulnerabilities in the container hosting the web app are dealt with during monthly updates. Severe CVE alerts are patched immediately.
Do you have a bug bounty or responsible disclosure programme?	Information Security Policy available on request from info@leadingai.co.uk

7. Penetration Testing

Question	**Answer**
Do you conduct penetration testing and how often?	Penetration testing is done after each full release.
How quickly are measures put in place post pen test results?	Immediately. Necessary changes are made in a demo environment to ensure functionality is not broken before rolling out.

8. Data Sovereignty and Residency

Question	**Answer**
Do you guarantee that all customer data, including backups and logs, remains within the UK?	Yes, all data is stored and processed in the Azure UK South Region unless specifically requested otherwise from the customer.

9. Sub-processors and Third-Party Dependencies

Question	**Answer**
Do you use any third-party sub-processors to deliver your service?	No.
Are any sub-processors or support teams located outside the UK/EU?	N/A.
If so, can you provide a list of sub-processors and their roles?	N/A.
How do you vet and monitor the security of these sub-processors?	N/A.

10. Business Continuity and Disaster Recovery

Question	**Answer**
What is your Recovery Time Objective (RTO) and Recovery Point Objective (RPO)?	RTO is circa 1 hour. RPO: We would recover a working version of the tool but would lose chat history (previous prompts and responses contained in cosmosDB).
How often do you test your disaster recovery plans?	Our build is automated allowing recovery within a few hours.
Do you have geographically redundant systems?	Everything is hosted in the client's tenant and inherits your business continuity arrangements.

11. Software Development and Change Management

Question	**Answer**
How are changes to the platform tested and deployed?	Changes are tested in a sandbox environment before being rolled out to client environments with client agreement.

Do you provide advance notice of major changes or downtime?	Yes, any major changes are discussed with the client prior to being applied. Clients are notified of any known downtime.

12. Data Retention and Deletion

Question	**Answer**
What is your data retention policy?	Data is contained within the client's Microsoft Azure Tenant; data is deleted with a frequency determined by the client.
How do you ensure secure deletion of customer data upon contract termination or request?	The data is in the client's tenant; upon termination we lose access to it.
Can you provide a certificate of data destruction?	Yes, if requested before access to the tenant is rescinded.

13. Customer Responsibilities and Shared Responsibility Model

Question	**Answer**
What security responsibilities fall on the client vs. the provider?	Data is in the client's tenant; the web app inherits your security. Leading AI is responsible for ensuring our code is secure.
Do you provide documentation or guidance on how clients can configure the platform securely?	Terraform scripts can be provided if required.